WHAT IS CLAIMED IS

1. Method for discovery, inventory, and assessment of critical information in an organization, said critical information including electronic data on computers, said method comprising the steps of:

a) defining critical information
b) generating a policy containing critical information definition
c) distributing this critical information policy to each computer that has critical information
d) generating the inventory of information on each computer
e) assessing the criticality of information based on the criticality definition in step c above
f) generating a report of the assessment results
g) collection of assessment results from all computers
h) generating a report of assessment results

2. A method, according to claim 1, where the critical information is defined by signatures.

3. A method, according to claim 2, where signatures include tag signatures and content signatures.

4. A method, according to claim 3, where tag signatures include markers on the data files, such as file type, password protection, encryption.

5. A method, according to claim 3, where content signatures include strings within an information document and include generic signatures as well as functional signatures.

6. A method, according to claim 5, where generic content signatures apply across the organization and functional content signatures apply to specific functional groupings.

7. A method, according to claim 1, where information inventory includes collecting information about the computing device, attributes of the computing device, a list of data files on the computing device, and attributes on the data file.

8. A method according to claim 7, where attributes on the data file include size, creation time, usage time, encryption information, password information.

9. A method, according to claim 1, where the critical information may be identified by color coding the criticality level.

10. A method according to claim 1, where assessment of critical information is done by identifying signature match between the signature book generated by definition of critical information and the signature of information documents on the computing device being assessed.

11. A method, according to claim 10, where the signature comparison could be accomplished by methods such as pattern matching, neural networks, weighted matches.

12. A method, according to claim 10, where signature matching could be accomplished using existing applications resident on the computing device.

13. A method, according to claim 12, where an instance of an existing application is the Indexing service popularly available on Microsoft windows operating system devices.

14. A method, according to claim 1, where generation of assessment reports includes creating a local database of storing information about each information document assessed.

15. A method, according to claim 14, where the assessment report includes average criticality and distribution of critical information.

16. A method, according to claim 1, where results from assessment of computing devices can be collected and correlated to generate aggregated criticality reports.

17. An apparatus for discovery, inventory, and assessment of critical information, said critical information including electronic data on computers, comprises:

a centralized software manager running on a computing device that is used to define critical information, distribute criticality definitions, collect assessment reports, and generate assessment results to determine critical information;

distributed software on each computing device that contains data to be assessed that is used to generate an inventory of information, assess critical information

based on the criticality definition, generate a report of assessment, and send the results to the centralized software manager

18. An apparatus of claim 17, where the centralized software and distributed software communicate messages over a network

19. An apparatus according to claim 18, where the network could be an Ethernet, wireless, or dialup network and the messages may be encrypted.

20. An apparatus according to claim 17 where the criticality definition can be sent to the distributed software on a on-demand or periodic basis and where the results of assessment can be sent to the centralized manager on an on-demand or periodic basis.